Proof-of-Cat: Securing cryptographic systems using cat entropy

mario.havel@ethereum.org
https://proofof.cat

Abstract. Cryptography based on private keys or structured reference strings relies on the secure generation of a random number, which has always been a challenge in informatics as it requires a non-deterministic entropy input that can be acquired only from the outside world. Modern operating systems utilize various sources of entropy, such as peripheral devices, user activity, or hardware RNG modules. Proof-of-Cat proposes an alternative approach to generating random noise that is coming from nature and offers high security guarantees. Our method involves harvesting entropy from the unpredictable behavior of domesticated felines, also known as cats.

I. Introduction

With the exponential growth of computer systems and internet, cryptography plays a crucial role everywhere – from a daily life, to national security. In last few decades, asymmetric cryptography [1] enabled us to build free and open tools envisioned by cypherpunks. Elevating individual’s privacy, security and online freedom, these technologies have the potential to disrupt traditional power structures. But whether it’s a single key or public key cryptography, the security model depends on the randomness and unpredictability of the private key. As it should be difficult and practically impossible for an attacker to guess or derive the key from other information.

The generation of a truly random key has always been a challenge in informatics, as computers are deterministic devices that follow predefined instructions. To overcome limitation of pseudo-random numbers, modern operating systems rely on various sources of entropy that are external to the computer. These randomness sources are mostly extracted from peripheral devices by sampling user activity, such as mouse movements and keystrokes or variables like temperature or electrical noise.

The need for external sources of entropy extends beyond just the generation of private keys, nonces or salts. More than just encrypting and verifying data, advanced tools for enabling system privacy and scalability require further secure randomness inputs. Structured reference strings as used zero-knowledge cryptography or homomorphic encryption requires a good amount of randomness. It’s important to keep in mind that all of the ecosystem built on top of the base layer of randomness inherits its security.

II. Proof-of-Cat: A novel approach to secure cryptography

Proof-of-Cat proposes an alternative approach to generating random noise for cryptographic systems, utilizing the inherent unpredictability and randomness of domestic felines, also known as cats. Cats are known for unpredictability in their behavior, as they are highly sensitive to their environment and can react differently to the same stimuli at different times [2]. This innate chaos makes them an excellent source of entropy for cryptographic systems.

III. How are cats a good source of entropy

In many societies, collective consciousness would agree that cats fall into chaotic good category. The intrinsic unpredictability of their behavior is a one reason for considering them as an entropy input. Even in field of chaos theory itself, we find acknowledgment of cat chaos in the Arnold's cat map transformation. Truly exhibit of a sensitive dependence on initial conditions.

In addition to their inborn unpredictability, cats also have a high level of quantum information entropy. The amount of uncertainty associated with the state of a quantum system is a concept similar to the classical notion of entropy but with the added complexity of quantum mechanics. It has been shown that cat-like states that exhibit a high level of quantum information entropy [3]. Indicating a high degree of chaos and unpredictability in quantum world however doesn’t have to imply chaotic nature of domestic cats. Or maybe these cats lead to ToE beyond the standard model?

As these statements tend to generalize, it’s important to note that quality of entropy depended on a given cat. Degree of entropy generated by a cat can be influenced by many factors like age, level of domestication, feline breed, etc. For example, we can expect lower randomness output from chonky bois and other lazy kind of kitties.

With that in mind, we can also establish that using cats as an entropy source would benefit from adding more cats into the computation. Their individualistic behavior creating significant differences between cat data with a proper entropy extraction algorithm would contribute to overall higher entropy.

The level of entropy in a cat can also be increased through the use of stimuli, such as cat toys, treats or red dot delusion [4]. Reaction can vary a lot because of chaotic cat nature. And by introducing these stimuli at random intervals, the behavior of the cat becomes even more unpredictable, leading to a higher level of entropy.

Mentioning this option, it is important to remember to always treat cats with respect and not overstimulate them. Cats with their own unique personalities and preferences are independent beings and it’s important to treat them as such. In safe and enriching environment, with their needs and comfort level satisfied, we can help ensure that our feline friends remain happy, healthy and chaotic.

IV. Harvesting cat entropy

For extracting cat entropy for cryptographic systems, we must consider its hardware and software solution. Hardware for harvesting the entropy must be non-invasive and always fully safe for the cat. This still leaves many options how to get the purrest randomness.

The first theoretical way is to use sensors to monitor the movements and actions of a cat, such as the movement of its paws, tail, or head. Sensors can be attached to the cat in a non-invasive manner, such as through the use of a collar or harness. By collecting data from various parts of the kitty, we might achieve a lot of data since each movement has different patterns.

However, from a feasibility perspective, this solution would not be very practical. It is not easy to attach one sensor to a cat, not even talking about multiple ones. Cats used to wearing a collar might tolerate a relatively small object hanging from it. Yet, this limits the entropy generation only to certain kind of collar wearing cats and still has a high risk of getting damaged or stolen.

Another, more feasible approach, would be to use cameras to track the cat's movements. Using entropy of a video is not a novelty in generating secure random numbers but using Proof-of-Cat, it might become cheaper and more accessible. Instead of buying shitton of lava lamps, we can support existing cat colonies, shelters or even befriend a local *cat lady*. In addition to the video output, system using cats can even utilize the sound to produce, literally, the purrest entropy.

The data collected from cameras will take significantly more space, making it more expensive while not providing much more randomness than just movement data.

Next proposed solution is the most practically tested one. Device developed under the codename *Catropy* is a dedicated cat toy for collecting randomness, creating the first cat hardware randomness generator (CHRNG).

In contrast to previous proposals, an independent toy collecting movement (or potentially other) data offers various advantages. It doesn't have to be attached to the cat, it gives the cat and the owner much more freedom in its usage. As a toy, it itself can serve as a stimuli to improve cat's randomness output, as described above. A soft, preferably fluffy, coating of the toy provides enough hardware security from all those frisky kitties.

The hardware part itself consists of a small microcontroller and sensors like gyroscope and accelerometer. Cheap and miniaturized device with open source design would allow anyone to utilize their cat as a secure randomness generator. Computational capacity of the microcontroller gives us many options to further manipulate and extract entropy.

On the software side, we can use Shannon entropy to determine the quality of the entropy output. When it reaches value considered secure, raw entropy still shouldn't be accessed directly but processed using extractor chaos function. The final output, properly extracted and encoded can be read directly by connecting the board to computer via serial port, USB or even wireless if further encryption needs are met.

V. Advantages of Proof-of-Cat

Based on purpose of its use, Proof-of-Cat can offer various advantages over traditional sources of entropy. First and foremost, it utilizes an ecological, widely available and purely natural source of entropy that is unpredictable and random. This makes the approach affordable, easy to use while making it asymmetrically difficult for a potential attacker to derive the key, as the behavior of cats is practically impossible to predict or reproduce.

In addition, the use of cat entropy can also help reduce the reliance on potentially compromised sources of entropy in widespread consumer devices. This can further improve security of an individual or strengthen the security model of a cryptographic system.

Last but not least, it's certainly the cutest source of entropy.

VI. Potential attacks on Proof-of-Cat

Like any other system, Proof-of-Cat is not invulnerable to attacks. Nonetheless, attacks on cat entropy might be very expensive making them impractical for most of the cases.

For example, an attack trying to control behavior of a cat would require either large amount of effort to train a cat. Some people indeed consider it possible to train a cat but it still requires a lot of time and more importantly, agreement of the cat. Cat needs to want to be trained. Especially in case of insidious attackers like government agencies, we can be pretty pretty sure that cats don't like to cooperate with the state. (Fig. 1)

Another potential attack to control cat's behavior might be using hardware devices. A robotic cat exoskeleton could be build and used to guide it's moves. Nevertheless, it would be pretty expensive and also obvious that your poor cat is controlled by an alien robot.

In terms of predicting cats behavior, another potential attack is the use of a machine learning algorithm to learn and predict the behavior of the cat. If an attacker is able to accurately predict the behavior of the cat, they may be able to derive the key or introduce bias into the randomness generator. This can be mitigated by using more cats as it gets exponentially more complicated to predict their behavior. And if we have an AI or supercomputer which can do that with hundreds of cats, we are fucked anyway.

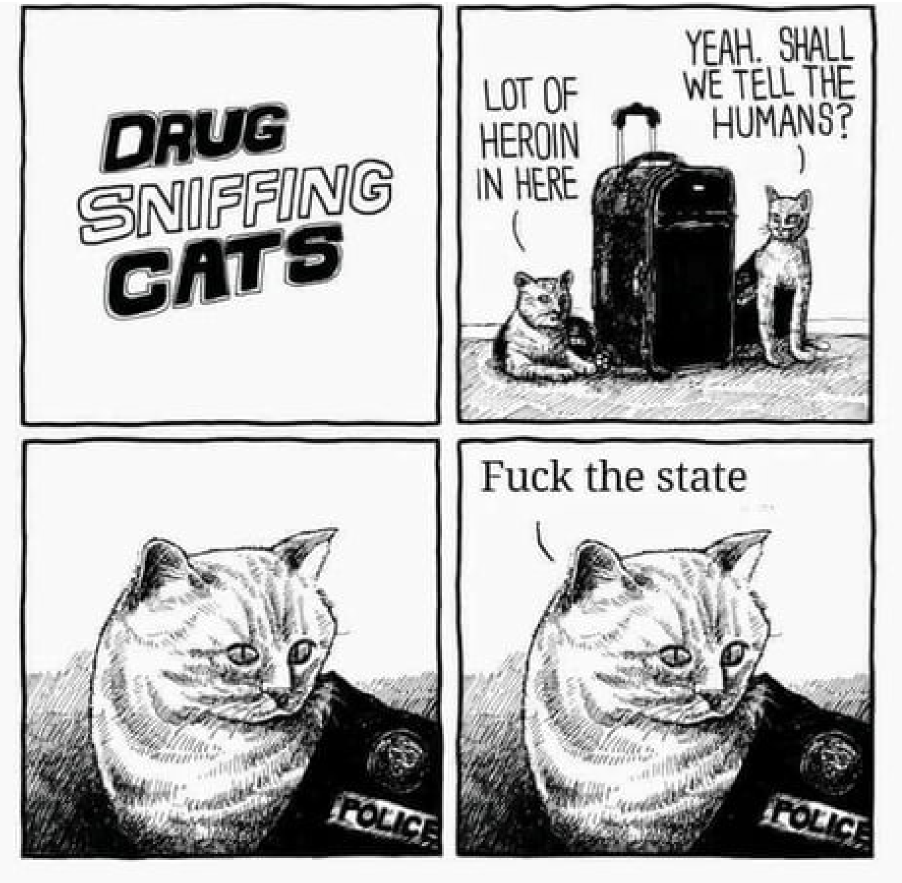

Figure 1: Cats are anarchists

From the hardware perspective, a potential attack is the compromise of the sensors or cameras used to harvest cat entropy. An attacker could potentially manipulate the data collected by the sensors or cameras.

To mitigate these attacks, it is important to make sure the sensors have not been tempered with, as well as continuously monitor the behavior of the cat to ensure that it remains unpredictable. Use of multiple cats is also strongly advised.

VII. Conclusion

Proof-of-Cat is a promising and innovative method for generating random noise for cryptographic systems. By harnessing the inherent unpredictability and randomness of domestic felines, this approach has the potential to offer affordable security for various cryptography usecases.

While some implementations of Proof-of-Cat proposed in this paper have been partially or fully tested, there is still a need for further research and development in order to fully understand the capabilities and potential of this approach. This may include exploring its feasibility for use in a wider range of practical applications, as well as identifying any potential limitations or challenges that may arise. Overall, Proof-of-Cat is a unique and intriguing concept that has the potential to bridge

References

[1] Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. https://ieeexplore.ieee.org/document/1055638

[2] Turner, D.C., & Bateson, P.P.G. (2000). The Domestic Cat: The Biology of its Behaviour (3rd ed.). Cambridge University Press. ISBN 9781107025028.

[3] Miranowicz, A., Bajer, J., Wahiddin, M. R. B., & Imoto, N. (2001). Wehrl information entropy and phase distributions of Schrodinger cat and cat-like states. https://arxiv.org/abs/quant-ph/0107107

[4] Armstrong, E., Chester (2021, May). My cat Chester's dynamical systems analysis of the laser pointer and the red dot on the wall: correlation, causation, or SARS-Cov-2 hallucination? https://arxiv.org/abs/2103.17058